THOSE PESKY* "GOVERNMENT" "RECORDS": DATA RESERVATION AND STORAGE TO HELP YOU AND YOUR COUNTY AVOID SPOLIATION CLAIMS

* DISCLAIMER: They aren't really "pesky" at all; they do matter a heck of a lot, though, and the ALL THE RULES governing them matter just as much

TOPICS TO COVER

- Understanding Your Duty to Preserve Government Records
  - GRAMA
  - Litigation Holds
- Understanding Your Data Storage: Where and by Whom
- Understanding the Type of Data You Maintain
- Case Study: Salt Lake County's Data Breach

SCOPE OF THE COUNTY'S DUTY: UTAH GOVERNMENTAL RECORDS ACCESS AND MANAGEMENT ACT ("GRAMA")

LEGISLATIVE INTENT

- 63G-2-102. Legislative intent.
- (1) In enacting this act, the Legislature recognizes two constitutional rights:
  - (a) the public's right of access to information concerning the conduct of the public's business; and
  - (b) the right of privacy in relation to personal data gathered by governmental entities.
- (2) The Legislature also recognizes a public policy interest in allowing a government to restrict access to certain records, as specified in this chapter, for the public good.

LEGISLATIVE INTENT (CONT.)

- The opening paragraphs further state legislative intent to:
  - promote the public's right of easy and reasonable access to public records;
  - specify the conditions under which the public interest in allowing restrictions on access to records may outweigh the public's interest in access;
  - prevent abuse of confidentiality by governmental entities;
  - provide guidelines for both disclosure and restrictions on access to government records, which are based on the equitable weighing of the pertinent interests and consistent with nationwide standards of information practices;
  - favor public access when countervailing interests are of equal weight; and
  - establish fair and reasonable records management practices.

WHAT IS A "RECORD"?

- 63G-2-103. Definitions. . . . .
- (22) (a) "Record" means a book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material regardless of physical form or characteristics:
  - (i) that is prepared, owned, received, or retained by a governmental entity or political subdivision; and
  - (ii) where all of the information in the original is reproducible by photocopy or other mechanical or electronic means

IMPORTANT: Format is not a factor; content, not format, is what is important in determining a record.

IMPORTANT: Location is not a factor; content, not location, is what matters.

YES, THAT CAN INCLUDE PERSONAL E-MAIL ACCOUNTS AND MOBILE TELEPHONES.

WHAT IS A "RECORD"? (CONT.)

YES, THAT CAN INCLUDE PERSONAL E-MAIL ACCOUNTS AND MOBILE TELEPHONES!

WHAT IS A “RECORD”?

- 63G-2-103. Definitions. . . . .
- (22) (b) "Record" does not mean:
  - (i) a personal note or personal communication prepared or received by an employee or officer of a governmental entity:
    - (A) in a capacity other than the employee's or officer's governmental capacity; or
    - (B) that is unrelated to the conduct of the public's business;
  - (ii) a temporary draft or similar material prepared for the originator's personal use or prepared by the originator for the personal use of an individual for whom the originator is working;
  - (iii) material that is legally owned by an individual in the individual's private capacity . . . .
  - (ix) a daily calendar or other personal note prepared by the originator for the originator's personal use or for the personal use of an individual for whom the originator is working;

WRITTEN REQUEST REQUIRED

- 63G-2-204. Requests -- Time limit for response and extraordinary circumstances. . . . .
  - (1) A person making a request for a record shall furnish the governmental entity with a written request containing:
    - (a) the person's name, mailing address, and daytime telephone number, if available; and
    - (b) a description of the record requested that identifies the record with reasonable specificity. (Emphasis added.)

IMPORTANT: "Reasonable specificity" can matter, especially in requests for e-mail. Compare "all e-mails between Elected Official and Staff 1-4 from January 2013 to present" with "all e-mails to or from Elected Official and Staff 1-4 discussing Main Street road project in August 2014."

REASONABLE TIME TO RESPOND

- 63G-2-204. Requests – Time limit for response and extraordinary circumstances.
  . . . .
- (3) After receiving a request for a record, a governmental entity shall . . . .
  - (b)(i) approve the request and provide a copy of the record;
  - (ii) deny the request in accordance with the procedures and requirements of Section 63G-2-205;
  - (iii) notify the requester that it does not maintain the record requested and provide, if known, the name and address of the governmental entity that does maintain the record; or
  - (iv) notify the requester that because of one of the extraordinary circumstances listed in Subsection (5), it cannot immediately approve or deny the request, and include with the notice:
    - (A) a description of the circumstances that constitute the extraordinary circumstances; and
    - (B) the date when the records will be available, consistent with the requirements of Subsection (6).

IMPORTANT: This can be superceded by ordinance or policy; in SLCo, for example, ordinance requires we produce documents as soon as possible but no more than 10 business days (5 for media requests).

WHAT COUNTS AS "EXTRAORDINARY"?

- 63G-2-204. Requests – Time limit for response and extraordinary circumstances.
  . . . .
- (5) The following circumstances constitute "extraordinary circumstances" that allow a governmental entity to delay approval or denial by an additional period of time as specified in Subsection (6) if the governmental entity determines that due to the extraordinary circumstances it cannot respond within the time limits provided in Subsection (3):
  - (c)(i) the request is for a voluminous quantity of records or a record series containing a substantial number of records; or (ii) the requester seeks a substantial number of records or records series in requests filed within five working days of each other . . .
  - (e) the request requires the governmental entity to review a large number of records to locate the records requested;
  - (f) the decision to release a record involves legal issues that require the governmental entity to seek legal counsel for the analysis of statutes, rules, ordinances, regulations, or case law;
  - (g) segregating information that the requester is entitled to inspect from information that the requester is not entitled to inspect requires extensive editing . . .

  IMPORTANT: With large e-mail requests, sometimes all 4 of these will come into play.

"NO" CAN PRETTY MUCH NEVER BE THE ANSWER

- Again, "A public record is a record that is not private, controlled, or protected and that is not exempt from disclosure; therefore, all records are public unless expressly restricted by law." (Emphasis added.) 63G-2-103(21).
- Also, access to records may not be hindered by its format. A governmental entity must be able to provide for proper public inspection and copy of public records even if they are electronic.
  - Subsection 63G-2-201. Right to inspect records and receive copies of records. . .
    - (11) A governmental entity may not use the physical form, electronic or otherwise, in which a record is stored to deny, or unreasonably hinder the rights of a person to inspect and receive a copy of a record under this chapter.
- Segregation is the preferred treatment when a record contains both public information (that requestor is entitled to inspect) and private/controlled/protected information (that requestor is not entitled to inspect). 63-G-2-308.

BUT "YES, AND IT WILL COST YOU" MIGHT BE

- GRAMA states that a governmental entity may charge a reasonable fee to cover the actual cost of providing a record.
- 63G-2-203. Fees. . . . .
  - (1) A governmental entity may charge a reasonable fee to cover the governmental entity's actual cost of providing a record. This fee shall be approved by the governmental entity's executive officer.
  - (2) (a) When a governmental entity compiles a record in a form other than that normally maintained by the governmental entity, the actual costs under this section may include the following:
    - (i) the cost of staff time for compiling, formatting, manipulating, packaging, summarizing, or tailoring the record either into an organization or media to meet the person's request;
    - (ii) the cost of staff time for search, retrieval, and other direct administrative costs for complying with a request; and
    - (iii) in the case of fees for a record that is the result of computer output other than word processing, the actual incremental cost of providing the electronic services and products together with a reasonable portion of the costs associated with formatting or interfacing the information for particular users, and the administrative costs as set forth in Subsections (2)(a)(i) and (ii).

IMPORTANT: Fees cannot include the cost a reviewing a record to determine whether it is subject to disclosure (63G-2-203(5)(a)), unless allowed by subsection 2(a)(ii) above.

WELL, THAT'S SUB-OPTIMAL. SUGGESTIONS?

- I like to incorporate civil discovery practices into my GRAMA practice anyway, so I tend to:
  - Negotiate terms and parameters.
    - Negotiate e-mail request from "all e-mails between Elected Official and Staff 1-4 from January 2013 to present" to either "all e-mails to or from Elected Official and Staff 1-2 discussing Main Street road project in August 2014" or "all e-mails to or from Elected Official and Staff 1-2 containing the following key terms: "main street," "[contractor name], " or "[contract number]."
    - Explain exactly what they are asking for and see if that's really what they want or if they can do with less. E.g., request for "all body camera footage" (60+ cameras) versus "body camera footage for two officers involved."
  - Consider discussing and refining the request even if they've asked for a non-record. Example, "a list of all Assessor's Office employees subjected to any form of discipline from 2012 to the present." It's probably easier to create the list than wait for the follow up request for "records sufficient to show all employees . . . ." (Note: also negotiate "discipline' and include the negotiated terms in the production letter.)

SUGGESTIONS (CONT.)

- Be up front with realistic timelines and anticipated costs, with enough detail to explain both that the requestor can make an informed decision whether to refine her request.
  - For example, in the mugshots.com case we were very clear how long fulfilling a request would take, based on a test sample, and how much it would cost both at the minimum rate (least expensive employee) and the anticipated higher rate ("extensive records request" fees). Remember: it helps to be consistent!
- Be very specific with partial denials or additional information you think might be helpful on appeal.
  - Bates stamp the production and note the Bates ranges applicable to each request in the production letter.
  - Disclose where you looked and where you didn't (e.g., personal cell phones or e-mail accounts), or where you let the subject search herself due to significant privacy concerns (e.g., ditto).

SCOPE OF THE COUNTY'S DUTY: LITIGATION HOLDS

- **In litigation, the scope of a party's duty to preserve is coterminous with the scope of discovery.**
  - Fed. R. Civ. P. 26(b)(1): "Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense."
    - NOTE: not just claims, but also defenses (of both the County and the plaintiff)
  - Utah R. Civ. P. 26(b)(1): "Parties may discover any matter, not privileged, which is relevant to the claim or defense of any party if the discovery satisfies the standards of proportionality set forth below."
    - Factors include whether the discovery is "reasonable, considering the needs of the case, the amount in controversy, the complexity of the case, the parties' resources, the importance of the issues, and the importance of the discovery in resolving the issues"; whether "the likely benefits of the proposed discovery outweigh the burden or expense"; and whether "the information cannot be obtained from another source that is more convenient, less burdensome or less expensive."

SCOPE OF THE COUNTY'S DUTY: OTHER

- **Third-party subpoenas:**
  - Duty is owed to the issuing court.
  - Scope of the duty is coterminous with the subject as described on the face of the subpoena.
    - Note: If you know or suspect that more will be relevant than what is described in the subpoena, consider broader hold sooner rather than later.
- **Regulatory requests or "informal" investigations:**
  - Duty is owed to the government, not a court, to carry out the mission of the agency.
  - Scope of the duty is based on information known at the time the duty is triggered, and may change over time as additional facts become known.
    - Again: If you know or suspect that more will be relevant than what is described in the request, consider broader hold sooner rather than later.

WHAT TRIGGERS THE DUTY TO PRESERVE?

- The duty to preserve documents and information arises as soon as litigation is "reasonably anticipated," "reasonably foreseeable," or "reasonably likely."
- The trick is knowing when the triggering event has occurred and then thinking through all the claims and defenses relevant to that trigger.
  - Your understanding of the "trigger" and its scope may change as new facts are discovered.
  - Remember to update your analysis as new facts come up.
    - Example: The County terminates an employee (TE1) for excessive tardiness and poor work quality. TE1 threatens to sue. You preserve TE1's personnel file, time sheets, and the supervisor's notes regarding TE1's time and performance. While investigating the claim, you learn that another employee accused TE1 of misusing her County e-mail. You broaden the litigation hold to encompass TE1's County e-mail account and all documents pertaining to complaints about it.
      - Remember: with terminated employees, automatic deletions often occur quickly. With "noisy" or "VIP" terminations, consider preserving early.

WHAT TRIGGERS THE DUTY TO PRESERVE? (CONT.)

- **Bright line triggers:**
  - Service of a complaint or Notice of Claim
  - Service of a third-party subpoena
  - Receipt of an investigative demand or inquiry (even informal)
- **"Gray line" triggers:**
  - Representation letters or preservation demands from claimants or counsel
    - Tone and author of letters, complaints, etc.
    - "I will sue you" v. "we are deciding whether to sue you"
    - "I will sue you unless you do X" v. "If you don't do X, I will consult an attorney"
  - Employee complaint, "I'll sue you!"
  - Whistleblower allegations (varies based on results of investigation)
  - Whether these trigger the duty will depend on the facts and circumstances.

WHAT TRIGGERS THE DUTY TO PRESERVE? (CONT.)

- **"Use your best judgment" triggers:**
  - These are the hardest because they are triggered based on your own judgment, rather than the act of a third party (e.g., filing a complaint or serving a Notice of Claim).
  - Fires, explosions, serious auto accidents, deaths, etc.—usually considered triggers warranting a litigation hold.
  - Slip and falls, minor injuries or minor property damage (e.g., a snow plow hits a mailbox), etc.—usually not considered triggers.
  - Key is to analyze all the facts, including your prior experiences, and reach a reasonable conclusion about the best course of action.
    - Often better to err on the side of preservation, unless there is good reason not to (e.g., proportionality)
    - If you decide no hold is necessary, document your conclusion so that, if challenged later, you can defend it.

WHAT IF YOU FAIL TO PRESERVE RECORDS?:
STANDARDS FOR LIABILITY ON SPOLIATION CLAIMS

- Tenth Circuit: "Spoliation sanctions are proper when (1) a party has a duty to preserve evidence because it knew, or should have known, that litigation was eminent and (2) the adverse party was prejudiced by the destruction of the evidence. But if the aggrieved party seeks an adverse inference to remedy the spoliation, it must also prove bad faith. Mere negligence in losing or destroying records is not enough because it does not support an inference of consciousness of a weak case. Without a showing of bad faith a district court may only impose lesser sanctions." *Turner v. Public Serv. Co.*, 563 F.3d 1136 (10th Cir. 2009).

BEST PRACTICES WHEN PRESERVING RECORDS

- If in doubt, get guidance; brainstorming with colleagues never hurt anyone.
- Ask your county attorney's office to research the substantive case law to make sure they understand all the legal nuances
- Practice tip: Always ask your lawyer to look for GRAMA requests relating to the threatened litigation
  - You get a better idea what opposing counsel is thinking, AND
  - You get a better idea what opposing counsel already knows
- Practice tip: Always remember to release the hold
  - Pitfalls of failing to release the hold
  - Not an excuse to delete willy nilly

UNDERSTANDING YOUR DATA STORAGE

- Think about the systems you use. Is your data contained within your county on your own servers? Or do you allow third party hosting of data?
- Do you host data in the cloud or have third party storage of data?
- Do you use any internet based databases?
- If you have external data, do you have up to date contact information for these service providers?
- Do your third party providers have strict security requirements for securing your data?

KNOWING WHERE YOUR DOCUMENTS ARE STORED: WHAT IS CLOUD STORAGE?

- Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the Internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider.

- Put simply: You are “renting” space from someone else’s IT infrastructure, and you access that space via the World Wide Web (internet).

LEADING CLOUD STORAGE PROVIDERS

- Microsoft OneDrive;
- DropBox;
- Google Drive;
- Amazon Cloud Drive;
- Box.com;
- Apple iCloud;
- Mega Cloud Storage (founded by the infamous Kim Dotcom);

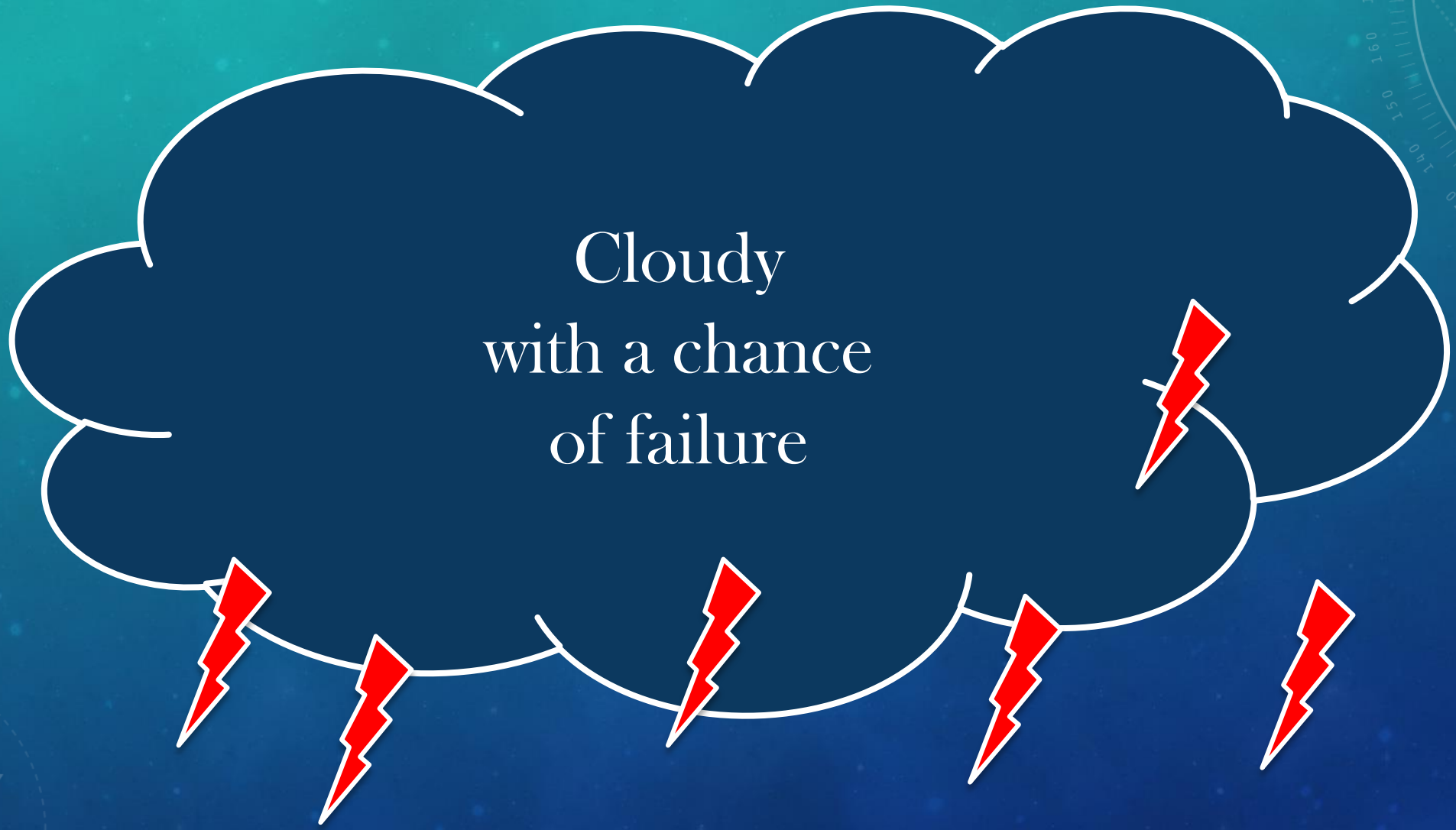
PROS OF USING THE LEADING CLOUD STORAGE PROVIDERS:

- Free or minimal cost;
- Ability to share large files;
- Backup and sync files across multiple computers;
- Undelete things. Meaning when something is deleted, it merely is marked for deletion in the cloud and is retained by the service provider for x amount of time. Retention periods can be anywhere from an hour to months depending on the level of service purchased;
- No need to buy storage servers or enter into IT maintenance contracts;
- Access cloud-stored files remotely from your phone, work, or home (i.e., no need for Citrix (yuck) and the like).

MORE PROS:

- Microsoft OneDrive: offers 5 GB of free cloud storage with every Microsoft account;
- DropBox Basic: offers 2 GB of free cloud storage (can pay for additional space and features with other DropBox subscriptions);
- Google Drive: 15 GB free storage to use across all Google applications;
- Amazon Cloud Drive: free with any Amazon Prime subscription, offers 5 GB of storage;
- Box.com: $5.00/user/mo. “Starter” subscription, offers 100 GB secure storage;
- Apple iCloud: offers 5 GB of free storage with every iCloud account;
- Mega Cloud Storage Free Plan: offers 50 GB of free storage.

SECURITY CONCERNS

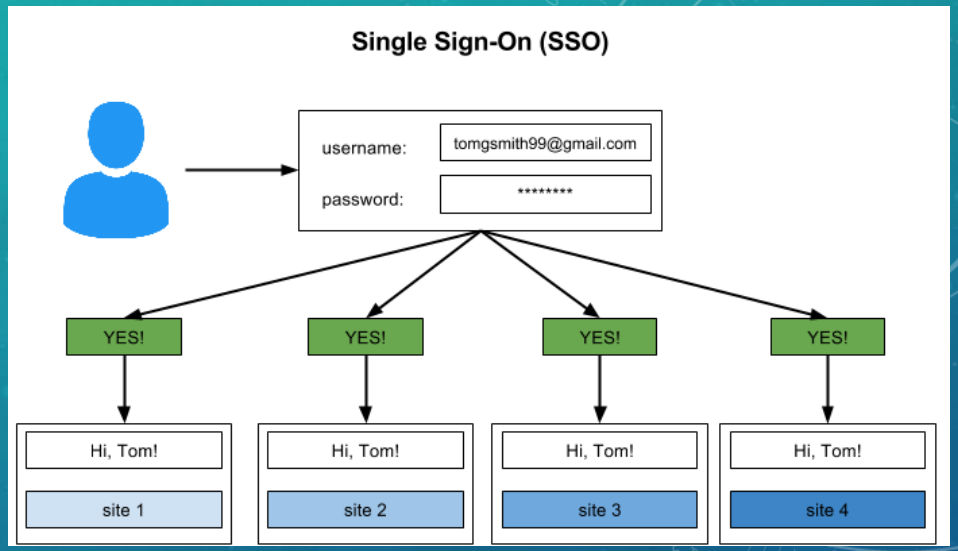


“MEMORY LEAKS”

- The cloud is a multi-tenant environment where resources are shared. Multiple entities can share the same server stack in the cloud, commonly separated by software that keeps the data separated.

- The software keeping data separated can become corrupt for multiple reasons, leading to data breach, including “memory leaks” where the software “wall” separating data between the multiple entities in the cloud becomes corrupt and leaks data from one entity’s account to another’s. This is a known risk in cloud storage and is why many government entities and hospitals choose not to use it.

SINGLE SIGN-ON (SSO)



- **Single sign-on (SSO)** is a property of access control of multiple related, but independent software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords.
- Single sign-on is a leading concern for systems such as Apple, Google and Microsoft, for which the same credentials (e-mail and password) are used for multiple systems (Gmail, Google Drive, Google Photos, Word Online, Office 365, OneDrive, iCloud, etc.). Meaning, your online account can be compromised simply by forgetting to log out.

UNDERSTAND THE TYPE OF DATA YOU MAINTAIN

- The law categorizes information into PII (Personal Identifying Information) and PHI (Personal Health Information) and HIPAA covered Information.
- Different regulations apply to each category of information
- State Laws (Utah)
  - Utah Code Ann. 13-44-101 et seq. (Protection of Personal Information Act)
  - Utah Code Ann. 26-33a-101 (Utah Health Data Authority Act)
- Federal Laws
  - HIPAA HITECH, Privacy and Security Rules (45 CFR 160)

PII (PERSONAL IDENTIFYING INFORMATION)

- PII relevant to a breach in Utah includes an individual's name with one or more of the following:
  - Social Security Number
  - Driver license or state issues identification card number
  - Account number or credit or debit card number in combination any security code, access code or password, etc. permitting access to the person's account.
- Data owners are responsible for breach reporting and notifications
- Limited methods of notification delivery
- You must notify the UT Data Owner immediately if breached
- Violations can result in heavy fines
- Data protection laws extend out-of-state
- See Utah Code Ann. 13-44-101 et seq. (Protection of Personal Information Act)

WHAT IS PHI (PROTECTED HEALTH INFORMATION)?

- **Protected health information (PHI)** under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" and can be linked to a specific individual. This includes any part of a patient's medical record or payment history.
  - Counties may have this information as it relates to services performed by their :
  - Health Department
  - Jail
  - County employees through their medical programs or Human resources
  - Other insurance programs (workers comp, life insurance, extended benefits)

PROTECTED HEALTH INFORMATION (PHI) INCLUDES THE FOLLOWING TYPES OF DATA:

- Name, social security, driver's license or ID number
- Phone number, fax number, email, URL or other web addresses
- Medical record numbers, account numbers, policy numbers
- Serial numbers, vehicle numbers,
- Biometric identifiers, fingerprints, retinal or voice prints
- Full face photographs or other comparable images

CASE STUDY: SALT LAKE COUNTY'S DATA BREACH

September 9, 2015

Salt Lake T

Friday, March 25, 2016

Salt Lake County data breac

Personal information of about 14,200 people — largely current and former Salt Lake County employees — was exposed for 75 days last summer, the district attorney's office has concluded.

But, thanks to a "white-hat hacker searching the Web for data that shouldn't be there," the illicit worker-compensation information apparently was pulled back before anyone else gained access to it, Jeff Rowley, risk manager for the district attorney's office, said in a report to the County Council this week.

"If we're going to have a breach," he added, "this is as good a breach as you can have."

County officials learned of the data breach on Sept. 9 after an industry trade publication, Modern Healthcare, reported 1.5 million records from California, Utah and Kansas were exposed starting June 18.

The breach occurred when Systema Software — a California company that provides claims-administration software to government agencies and private clients to handle worker compensation and auto and property insurance cl

SALT LAKE COUNTY'S DATA BREACH

- Notification of the breach
- Is this a hoax?
- What is a white hat hacker?
- Understanding the loss and securing the data
- Notifying affected parties
- Addressing the Press and GRAMA requests
- Multi-state reporting
- Credit monitoring services
- Silence

IF A BREACH OCCURS, WHAT ACTION IS REQUIRED:

- Secure your data and begin documenting the event
  - Documentation will be key to any loss recovery, insurance company demands and responding to media
- Understand the extent and manner of the data loss
  - In order to properly notify, you need to know what was lost.
- Notification
  After a determination regarding the scope of the breach and once reasonable integrity is restored to the system, the notification must be made in the most expedient time possible without unreasonable delay. An exception for delay is made if law enforcement indicates the notification may interfere with an investigation.
  - Be aware that other states use a different standard (risk of harm analysis). If there is a reasonable likelihood of harm then notification is required.

FINANCIAL COSTS

- Hundreds of staff hours
- $99,615.00 without staffing costs ($100,000 deductible)
  - Outside counsel
  - Outside PR firm experienced in responding to data breaches
  - IDT 911, plus additional credit monitoring
- Fully reimbursed by our outside vendor who handled the data

SO WHAT CAN WE DO?

- TALK TO YOUR IT PROFESSIONALS!
  - Plan ahead
    - Have a response team ready
    - Understand your data and data storage systems
    - Know your reporting responsibilities
    - Consider additional insurance coverage options
  - Discover and investigate all breaches of data
    - Secure your data
    - Send notification to affected persons
    - Offer identity theft protection
  - Make a public announcement and respond to news media, affected parties
  - Resume business

CYBER LIABILITY INSURANCE

- Coverage can provide:
  - Damages related to cyber losses
  - Breach Council
  - Credit monitoring services
  - Assistance with meeting notification requirements in all 50 states
  - Counsel related to media inquiries
  - Assistance with follow-up issues related to data retrieval

THANK YOU!

(Questions? Darcy M. Goddard, dgoddard@slco.org or 385.468.7761)

I'm no expert at the data storage side of things, but I hope this gives you some food for thought and a starting point for discussions with your IT professionals.